Information Assurance Requirements Brief

Marine Corps Systems Command
Information Assurance Division
Director

GGIBILISCO
2201
585

Information Assurance

Briefing Outline

- Information Assurance (IA) Division @ MCSC
- Terminology
- Certification & Accreditation (C&A)Process
- References

Information Assurance @ MCSC

Mission:

To support the implementation of Information Assurance (IA) policies and practices for the Marine Corps in its effort to develop and field systems and applications that ensure confidentiality, authentication, non-repudiation, integrity, and availability of information systems and applications.

Information Assurance @ MCSC

Charter

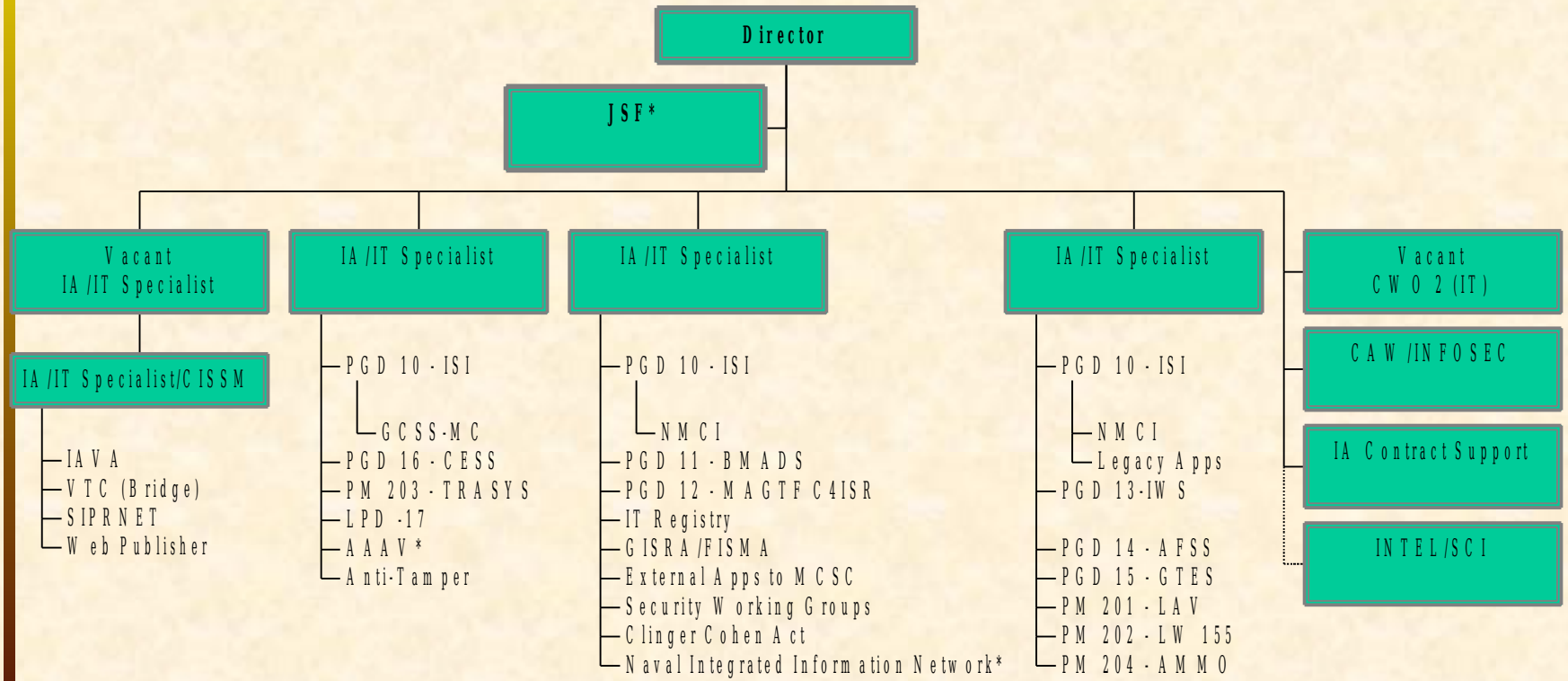
- To serve as the Commander's Independent Certification Authority (CA) for Security of Automated Information Systems
- To assist Project Officers in meeting DITSCAP documentation requirements
- To provide Certification Authority Workstation (CAW) implementation support
- To provide Information Assurance Vulnerability Alert (IAVA) reporting
- To provide Anti Tamper resource guidance
- To assist with Clinger Cohen Act documentation

Information Assurance @ MCSC

INFOSEC/COMSEC/C&A support for MAGTF C4I systems during

- Acquisition
- Implementation
- Fielding
- Life cycle support

Information Assurance @MCSC



*Denotes Special Programs

Information Assurance @ MCSC

- Program Manager Responsibilities:
  - Implement security requirements
  - Fund for SSAA/ASP development and Security Test & Evaluation (ST&E)
  - Provide IAVA POC for compliancy reporting

Terminology

- DITSCAP
- Certification
- Accreditation
- SSAA
- ASP
- CA
- DAA
- ATO
- IATO
- CCA
- C4ISP
- IAVA
- Anti Tamper

Terminology

DITSCAP

DoD Information Technology Security Certific
and Accreditation Process. All Automated Inf
resources, either tactical or strategic, used fo
collection, processing, maintenance, transmis
dissemination of information must comply wi
this process.

Terminology

CERTIFICATION

The comprehensive assessment of technical and non-technical security features of a system to establish the extent to which the particular design and implementation meets a set of security requirements.

Terminology

ACCREDITATION

A formal declaration by the Designated Approving Authority (DAA) that an automated information system is approved to operate in a particular security mode using a prescribed set of safeguards.

Terminology

SSAA

The System Security Authorization Agreement is the vehicle by which information is conveyed to the accreditation authorities.

The **SSAA is a living document that formalizes agreements regarding all accreditation requirements**.

Terminology

ASP

The Application Security Plan is a streamlined document that may be used in place of the SSAA when appropriate for less complex applications to achieve Certification & Accreditation.

Terminology

CA

The Certification Authority performs system security evaluations to establish adherence to specified security requirements and provides recommendations for certification and accreditation.

DAA

The Designated Approving Authority accredits the system to operate at an acceptable level of risk.

Terminology

ATO

Authority to Operate - The formal declaration by the DAA that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards.

IATO

Interim Authority to Operate - may be issued when the requirements for full Accreditation cannot be met. Must include a milestone plan with dates to achieve full Accreditation

Terminology

CCA

Clinger Cohen Act – compliance is required for all IT systems.

C4ISP

C4I Support Plan – Required for all programs that connect to communications infrastructure in any way. Used to facilitate integration and interoperability among C4I systems.

Terminology

IAVA

Information Assurance Vulnerability Alert – Reporting process is detailed on IA Website

Anti Tamper

System engineering activities intended to prevent and/or delay exploitation of critical technologies in US weapons systems. Part of Program Protection Plan (PPP) documentation.

C&A Process

The SSAA should be developed at Milestone A as part of the project officer's acquisition strategy.

Phase 1 - Definition of C&A level of effort

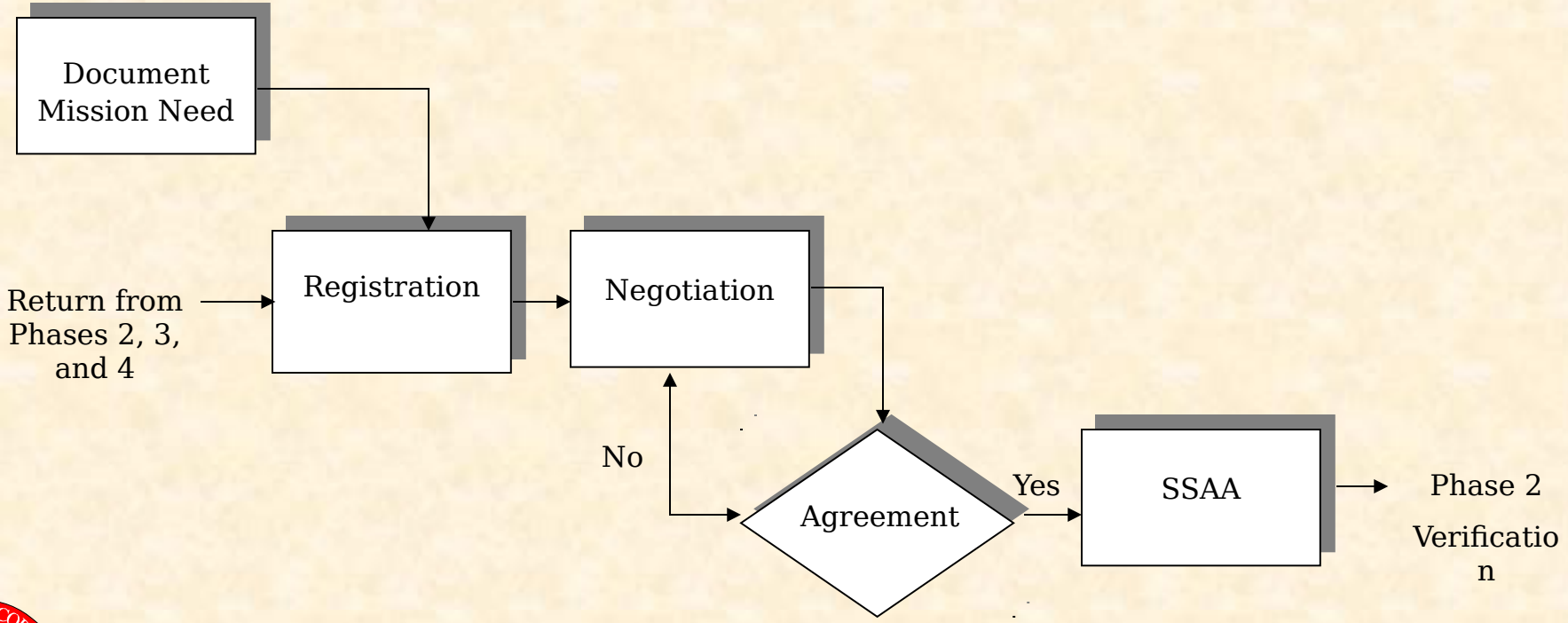
Phase 2 - Verification of system compliance with SSAA

Phase 3 - Validation of system accreditation

Phase 4 - Post Accreditation maintenance and operation

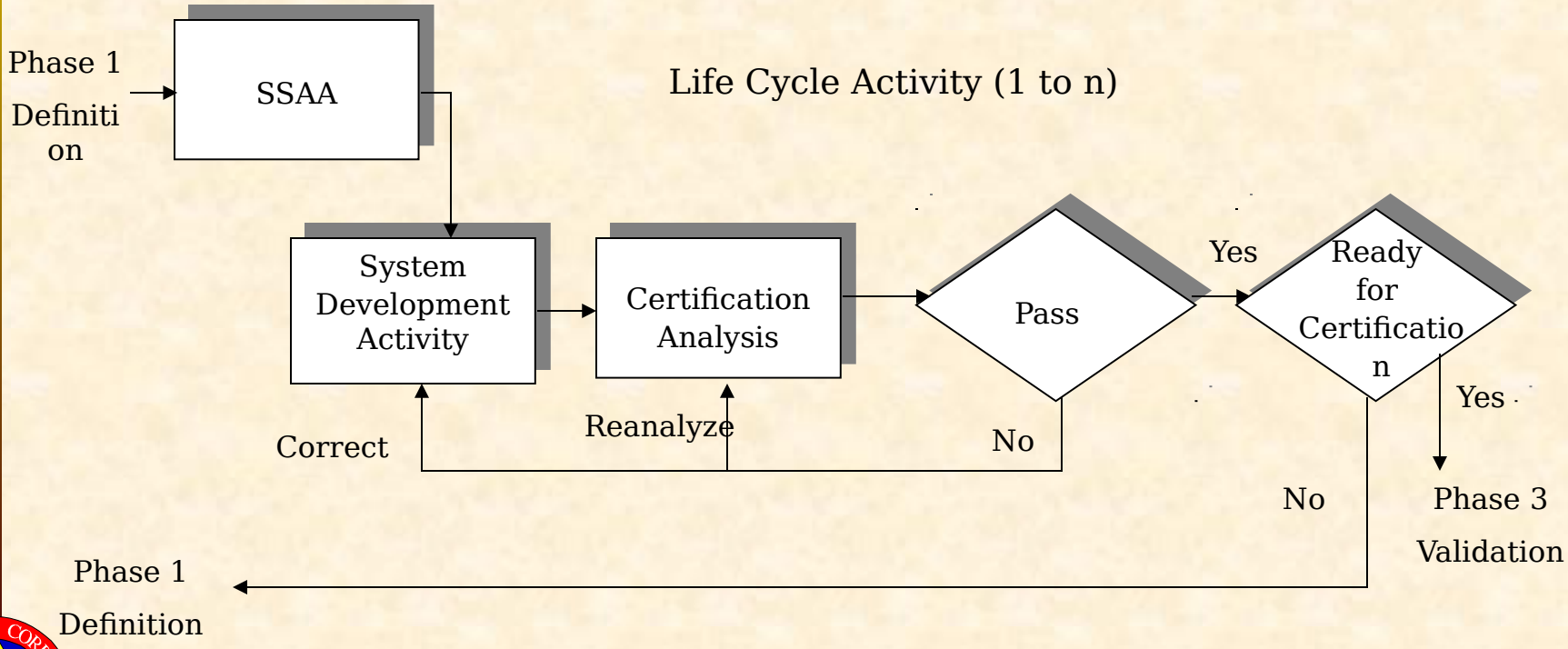
C&A Process

Phase 1: Definition



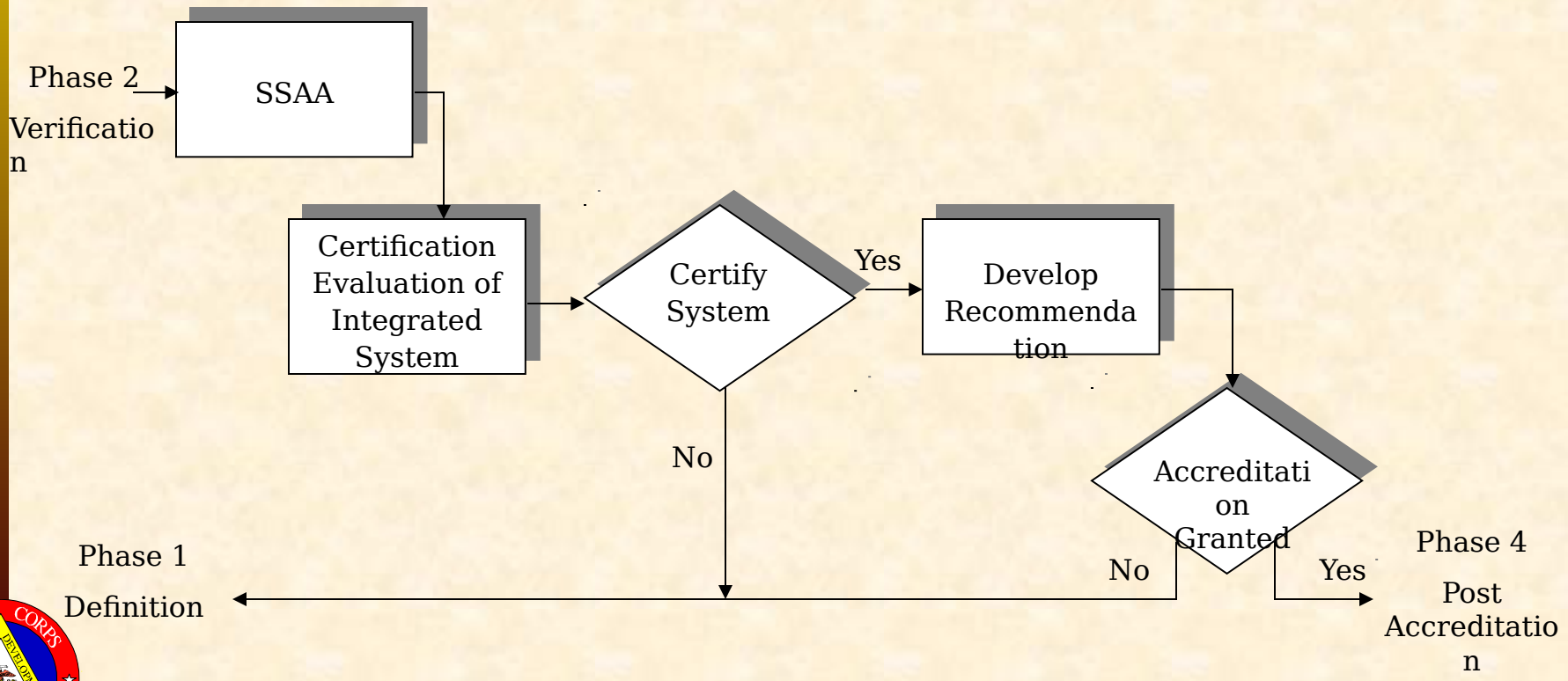
C&A Process

Phase 2: Verification



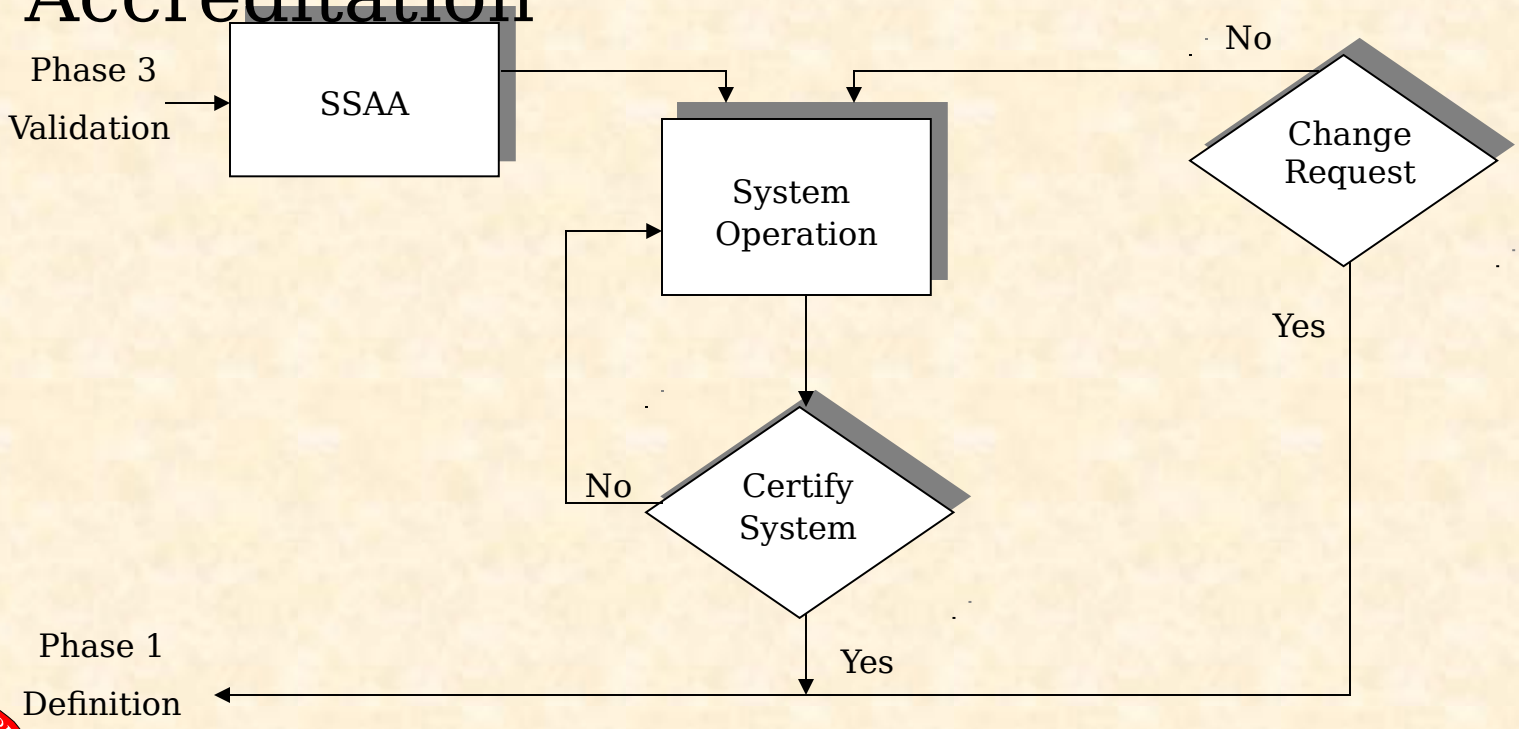
C&A Process

Phase 3: Validation



C&A Process

Phase 4: Post Accreditation



C&A Process

How do I start?

- **Register** your Program with the IA Division
- Include an IA Team Member on your IPT's
- Use the References and Templates on the IA Website http://www.marcorsyscom.usmc.mil/sites/ia

C&A Process

The PO will prepare an accreditation package with all required documentation and present it to the CA for review and staffing to the DAA. After reviewing the package, the CA will make a recommendation for the DAA to grant either:

- Authority to Operate (ATO)
- Interim Authority to Operate (IATO)
- Accreditation disapproval

C&A Process

The SSAA must be maintained throughout the system life cycle and must be updated every three years or whenever major software/hardware changes are made.

References

- DoDI 5200.40 (DITSCAP) http://infosec.navy.mil/DOCUMENTS
- 8510.1M DITSCAP Application Manual, July 2000
- SECNAVINST 5239.3 (DoN INFOSEC Program), July 1999 http://infosec.navy.mil/DOCUMENTS
- 8500.1 “Information Assurance”, October 24, 2000
- 8500.2 “Information Assurance Implementation”, February 6, 2003

References

- Commander ltr 5200 COS “Appointment as Designated Approving Authority (DAA)”, January 24, 2000
- MCO 5239.1, November 2002
- Deputy Commander, Marine Corps Systems Command ltr 5200 Ser C4ISR/156, 3 Sep 1999, Certification and Accreditation of C4ISR Systems
- Acreditview Database -request access through IA Website
- IA Quarterly Newsletter -Posted on *TIGER*; or send e-mail to ia@mcsc.usmc.mil to subscribe
- IA Website: http://www.marcorsyscom.usmc.mil/sites/ia

Information Assurance

Force Protection for the Information Warrior

Questions ?